Secure Search

Michael Raith (B.Sc.), *Student*

Abstract—Nowadays it is easy to track web users among websites: cookies, web bugs or browser fingerprints are very useful techniques to achieve this. The data collected can be used to derive a specific user profile. This information can be used by third parties to present personalized advertisements while surfing the web.

In addition a potential attacker could monitor all web traffic of an user e.g. its search queries. As a conclusion the attacker knows the intentions of the web user and of the company he is working for. As competitors maybe very interested in such information, this could lead to a new form of industrial espionage.

In this paper I present some of the techniques commonly used. I illustrate some problems caused by the usage of insecure transmission lines and compromised search engines. Some camouflage techniques presented may help to protect the web users identity.

This paper is a based on the lecture "Secure Systems" teached by Professor Walter Kriha at the Media University (HdM) Stuttgart.

Index Terms—secure search, search engine, client tracking, browser, cookies, web bug, geotargeting, IPv6, fingerprint, SSL, secure sockets layer, TLS, transport layer security, Tor Project, Startingpage, Firefox, NoScript, BetterPrivacy, Ghostery, GoogleSharing, HTTPS Everywhere, Ref Control

1 Introduction

In professional IT environments people are used to work in a multi level security zone system. This kind of security system allows an exact configuration for user authorization and access. Areas with secure content or client / server machines can be protected very well. Increases in network interconnectivity requires systems to be protected against connections from the network. This can be solved relatively easy in an Intranet. If you have in addition access from your Intranet to the Internet you must also protect your inner systems against the Internet. To accomplish this you can set up a proxy or firewall server to route all traffic to the Internet. There are well known concepts to solve these issues. Figure 1 gives an example DMZ[1] system setup as advised by the BSI [2].

Nowadays most enterprise systems are rather secure (with some exceptions ... [3, 4, 5, 6]). A bigger security risk since decades is induced by the human beens themselves with their short comings: short passwords, passwords saved in a text file on the desktop, insecure

michael.raith@hdm-stuttgart.de, Computer Science and Media (Master), Faculty Print and Media, Media University (Hochschule der Medien), Nobelstraße 10, D-70569 Stuttgart

1. **Dem**ilitarized **Z**one, see [1]

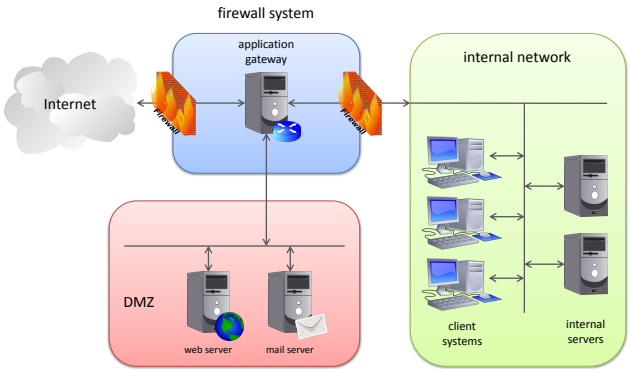


Fig. 1: example architecture – DMZ network with two firewalls

USB sticks, installation of insecure third party software, and so on ... these are only a few examples.

Study [7] about industrial espionage in the German economy proofs that theory. 18.9 % of the surveyed companies had already an industrial espionage. In 35.1 % of the cases there was a unconfirmed suspicion of industrial espionage. It turned out that 24 % of the offenders were employees of the companies themselves! Economic uncertainty, job losses, rising job pressure, and lack of appreciation of an employee may be the cause of industrial espionage and the runoff from business critical information.

> *Loyalty towards the employer is no longer taken for granted today. In some cases loss of pay is compensated with suplementary income. With modern communication media, it is prettey easy to pass sensitive data to well-paying recipients without being noticed by the company.*
> — [7, p. 25 (translated)]

Some employees are willing to harm their employer by selling sensible data to third parties. Another problem for loss of information is headhunting. A competitor could make a better salary offer and entice the employee away from its company. This happens with a probability of 18.1 %.

Hacker attacks against the IT as a reason of information loss are only listed at the third position with a percentage of 14.9 %.

64 % of all harmed companies had a financial loss between € 10 000 and € 1 million per liability case. Some companies (7.2 %) admit that they suffered a loss from

over € 1 million! Extrapolating these numbers for about 65 000 German companies, they [7, page 17] had come to an amount of loss of about € 2 800 million per year. The total loss is probably much higher, because they did not consider small business in their study.

Nowadays, I believe that there is a new form of industrial espionage. Web users are using search engines to query all kind of stuff without being aware what may happen at the background. Using some tricky techniques a user's company and his intentions can be identified. If a web user has an important position in a company for instance in management, research, or development, an attacker or spy of another company could gain advantage by observing the users web traffic.

The crux is, a search engine can see which search term the user is querying for and find out the user's location (e.g. country, city, company, research facility, university, ...). Also it is possible to determine a rarely used and unique search term. In addition the user's trace can also be tracked and logged over a lot of websites. Combining this information together, the search term, the user's location or company, and some websites the user was on, a profile about the user and the intentions of its company can be derived easily. If in addition the user is logged on at the search engine for supplemental services, it is much easier to get extra information. In case the provider of the search engine has an evil intention e.g. interests to sell the information and the drawn conclusions to third parties, this may lead to a new form of industrial espionage! Nobody knows for sure if this isn't already happening...

This scenario with the risk of an information theft can be achieved by the provider of a search engine (see Figure 2) or also in some ways by a man-in-the-middle attack (see Figure 3).

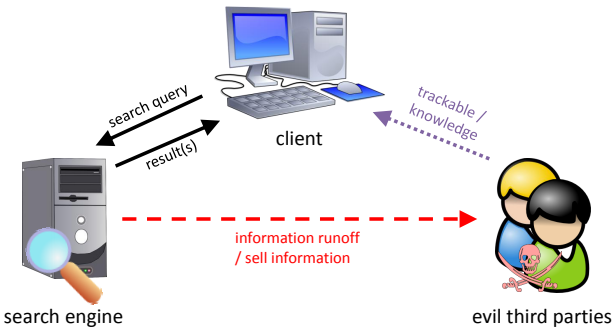


Fig. 2: information runoff by a search engine

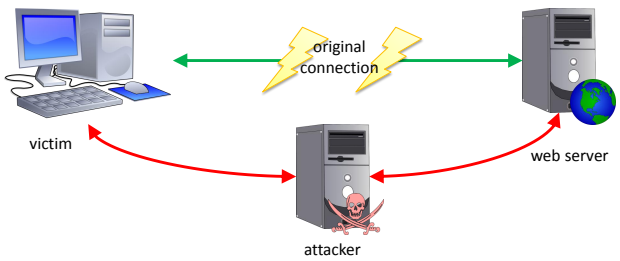


Fig. 3: man-in-the-middle attack

Some commonly used methods and techniques to track and monitor web site users are described in section 2. In section 3 I describe methods to protect Internet access against third parties and camouflage techniques for search queries.

2 Tracking Clients

An important issue on the web is that everybody is trackable in some ways. In the past users could be tracked easily with cookies. Nowadays, cookies are less used, because of restricted browser settings, growing awareness among users, and better web browser privacy controls. However, tracking is still possible with other methods like web bugs, fingerprints, or geotargeting. In the following subsections I will explain them in detail.

2.1 Cookies

The first specification of cookies was released in 1994. Since then cookies were used for useful things like sessions, but also for advertisements or persistent data storage at the client. A persistent cookie has a long expiration time. Such a cookie will be transferred each time the user requests content from that domain again.

An advertiser can track users over a lot of websites just by including advertisements into the website. While loading the advertisement a cookie with a random string will be stored at the client. On other websites advertisements from the same domain could be included. In this case the client will send his existing cookie back to the advertisment server. The server stores URL, date, and cookie in a log file. With that information the server (advertiser) can draw conclusions from the log file e.g. who you are, where you are, what you are looking for, what your interest are, to what social group you are belonging to and so on...

The vast proliferation of Flash made sure that so-called "Zombie-Cookies", "Local Shared Objects" (LSO) or "Flash Cookies" are increasingly gaining importance. Zombie-Cookies are created by the Flash player and stored in the file system; consequently the browser can not delete them any more. If the users tries to delete them, they usually will be recreated by the flash application automatically. Firefox has an extension called "BetterPrivacy" (see 3.3.2) which is able to automatically detect and delete such cookies.

Peter Eckersley states in [8] that "There is growing awareness among web users that HTTP cookies are a serious threat to privacy, and many people now block, limit or periodically delete them". Cookies and the traceability by third parties can be limited by disabling "third-party cookies" in the browser or by using a browser extension such as BetterPrivacy.

2.2 Web Bug alias Tracking Pixel

"Web Bug" is an synonym for a 1x1 blank tracking pixel [9]. These 1x1 pixels (usually PNG or GIF images) are included in a website or an HTML e-mail. While requesting the external image, the browser (or e-mail application) sends also some additional information to the server: the IP address of the requester, what kind of browser the requester has, the operating system, the requesting time, and a corresponding cookie (if available) of the same domain.

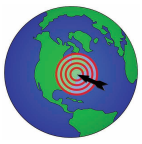
Therefore, third parties are able to check if an HTML e-mail was received, opened and potentially read. Web users can also be tracked and monitored among web sites. This technique is interesting for an advertiser as he is able to present personalized and invasive advertisements to the web user. They can also draw conclusions about relationships of products, websites, users, ethnic groups, etc.. A movement profile can be easily created from this data.

Some web bugs do not even require a cookie. It is possible to append information to a request without the usage of a cookie. If you want to know whether your spam e-mail has reached its target, you can insert a web bug and append the e-mail address of your target to the 1x1 pixel URL's end.

For example: the targets e-mail address is `foo@bar.baz` and the URL of the web bug `http://my-server.foo/web-bug.gif`. Combining this data you receive an extended URL like this: `http://my-server.foo/web-bug.gif?email=foo@bar.baz`. The URL extension `?email=foo@bar.baz` is ignored by the web server, but it's logged in a log file. Later, conclusions can be drawn easily by analysing the log files.

As you can see, the usage of web bugs is easy. Modern web bugs extend this functionality to other kinds of external resources e.g. scripts, stylesheets, or links. Blocking web bugs is not an easy thing to do since external resources are an important component of modern websites.

2.3 Geotargeting



Geotargeting [10] is a synonym for the determination of a web site user's geographical location to deliver different location based content. The granularity of location detection can be: country, region, state, city, street, organization, IP address, or ISP[2]. This technique is widely used for location based advertisements, news, and for restriction of video content for specific countries (e.g. legal or copyrights issues [11]). Some web sites use geotargeting to identify the users origin in order to present them the web site in their native language and, for example, to adapt the currency of a web shop.

Identification of the user's location via IP address is more or less the "old" way. As lots of people have a smartphone today, geographic identification of the user's location via GPRS or GPS is a "new" and more accurate way. Therefore, default activation of a smartphone's GPS module should be taken with care.

2. **I**nternet **S**ervice **P**rovider

2.4 IPv6

In 2011 the last IPv4 addresses will be exhausted [12]. Therefore IPv6 was developed which supports a factor of 2^{96} more addresses then IPv4. Everyone could now receive its own unique address. However, what does this mean for the users and the future of privacy? [13, 14]

The first part of the IPv6 address (the so called "prefix") is given by the provider. If he is not willing to change this prefix periodically, the user will be easily tracked and identified over a long period of time. This issue can become a serious privacy problem. The second part of the address (the identifier) will be protected: the "Privacy Extension" changes the interface identifier randomly and guarantees that a device address of an end device is not recognizable. An activation of this feature on every new system and device by default would be a good practice. Some new smartphones already have IPv6 support on board; currently there is no way to activate the "Privacy Extension" on some of these devices [15]. By default the identifiers are changed on those devices but in an inadequate manner.

Another concept of IPv6 is that every client in an Intranet system (behind a firewall or proxy) can also get its own IP address so no routers or NAT[3] is needed. These addresses can become visible in the Internet. This is a useful feature, but it can cause privacy and integrity problems particularly in big companies with a lot of clients.

IPv4 has the advantage that the provider forces a reconnection after a maximum of 24 hours. Therefore, the web user receives a new IP address every 24 hours latest. However, this feature will be abolished in regard to the article [16]. With IPv6 there will probably be no forced reconnection by the provider any more (only against some extra bucks!).

If the privacy will not be well-respected with IPv6, there will probably be no more anonymous users. ISPs or even governments would be able to accurately identify or track online users. Welcome surveillance society![4]

2.5 Browser Fingerprints

Nowadays it is easy to collect browser information. For each server request it appends e.g. the browser identification, what operating system it is running on, what rendering engine is used, and what file formats the browser accepts. With the help of JavaScript, Java, Flash or Silverlight even more data of interest can be determined. All this information combined yields something like a unique fingerprint for the web browser used.

3. **N**etwork **A**ddress **T**ranslation
4. Please keep in mind: This is a theoretical / "academic" work and should give you food for thoughts!

Browser fingerprints are a serious issue and should be taken with care. A team including *Peter Eckersley* did a study [8] for the *Electronic Frontier Foundation* to demonstrate how unique your web browser is in the world wide web. They ran a test with two groups of users: one group was conscious about privacy with special settings to camouflage their browser. The "normal" users had Adobe Flash or Java Virtual Machine as plugins enabled. 83.6 % of the privacy conscious users had a browser with an instantaneously unique fingerprint. The Browsers of "normal" users with plugins enabled showed an instantaneously unique fingerprint of 94.2 % [8, p. 2].

At the project's website http://panopticlick.eff.org/ you can test the uniqueness of your browser yourself. I performed the test with my Android 3.0 Tablet, Firefox 5.0 on a desktop PC with default settings and with the addon NoScript enabled. The browser on my Android tablet and my Firefox 5.0 with default settings seems to be unique among 1 675 384 tested browsers so far. Using Firefox 5.0 with the addon NoScript (see 3.3.1) enabled, only one in 16 425 had the same browser fingerprint. Running this test on your own system should give you some food for thoughts.

> *As a tracking mechanism for use against people who limit cookies, fingerprinting also has the insidious property that it may be much harder for investigators to detect than supercookie methods, since it leaves no persistent evidence of tagging on the user's computer.*
> — [8, p. 3]

A fingerprint with a wide diversity among others could be used as an "global identifier", because of its uniqueness. According to *Eckersley* a browser fingerprint can not easily be deleted such as a cookie. It requires major changes in browser settings to alter the fingerprint. A combination of browser fingerprints with the previously illustrated tracking methods may result in a serious threat regarding the user's privacy in the Internet.

> *Policymakers should start treating fingerprintable records as potentially personally identifiable [...]*
> — [8, p. 16]

3 Camouflage

A secure browsing experience can only be established by drawing a curtain over the requests or by camouflaging the user's browser. Some improvements can be achieved by changing the browser settings e.g. deactivate third party cookies. Some camouflage techniques requires specific effort. One option is to mask a browser's fingerprint in order to reduce its uniqueness in the internet (see 2.5). Another option is hiding your IP address.

Camouflaging the browser is possible but not always easy. In the following section I show some tools and techniques to establish a more secure browsing experience.

3.1 Secure Connections

A good starting point to protect the user (and his browser) against third parties is the usage of a secure connection. Nobody knows which route the packets between clients and servers take. Furthermore, the packets' route may change on every request and thus it is not possible to predict the route and its security. Proxys, routers, or other servers which route the packets to their destination can be compromised. This causes security issues regarding sensitive data e.g. credit card information. Consequently, a secure line for the transmission is required.

Today, you do not have to be in a high administrative position to get something like a red cable telephone for a secure transmission. Every browser since Netscape has the capability to establish a secure connection via SSL[5] (or the newer TLS[6]). The *Secure Sockets Layer* was designed as a separate protocol and therefore can be added as an extra layer to the protocols' architecture (see Figure 4).

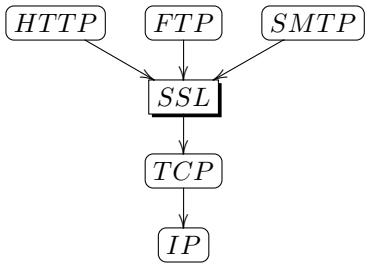


Fig. 4: SSL in the OSI model

The message is routed by the *Internet Protocol* (IP). Above is the *Transmission Control Protocol* (TCP), which provides a reliable communication. At the top there are application layer protocols e.g. HTTP[7], FTP[8] or SMTP[9]. SSL can be put between application layer and the regular transport layer. As a result, SSL is flexible enough to be used universally for different application layer protocols [17, p. 8].

There are also some disadvantages using SSL: first, a SSL certificate to authenticate the server against the client must be created and stored on a secure third party authentication server. Some older browsers also have a faulty behaviour if a SSL/TLS mode is not available: the browser switches back to a prior SSL/TLS

5. **S**ecure **S**ockets **L**ayer
6. **T**ransport **L**ayer **S**ecurity
7. **H**yper **T**ext **T**ransfer **P**rotocol
8. **F**ile **T**ransfer **P**rotocol
9. **S**imple **M**ail **T**ransfer **P**rotocol

version with bugs or may even use a non secure transmission without SSL. It is important to check the browser settings such that a non supported SSL/TLS connection is rejected instead of switching back to a non encrypted one. Another problem is that the server and client load rises due to extra SSL handshakes and (de-) compression of the data. Due to faster computers and networks this issue can be neglected nowadays.

Always keep in mind: a secure connection can only be established if the server offers one!

3.2 Using A Proxy

A server between two end-devices which forwards or filters data is called a proxy. This proxy can be configured to be transparent for end-devices. This allows to mask a end user client from a web server or a search engine. Setting up and configuring a proxy server is not an easy thing, hence I introduce two public proxy systems as examples. A third exemplary proxy system is introduced as a Firefox extension in 3.3.4 "Google-Sharing".

3.2.1 Tor Project

"Tor"[10] is a network to make the connection data anonymous. The service is based on the "onion routing" [19] principle. A message is encrypted repeatedly on consecutive network nodes (the message is wrapped in encrypted layers comparable to an onion skin). Each node only knows the previous and next nodes. Therefore origin, destination and content of the message is masked for the routing nodes.

The connection between two clients is always routed over three randomly chosen Tor nodes. The route is used for a period of time; afterwards new nodes are randomly chosen again. This guarantees that a route changes periodically and thus is not easily reproducible.

The entry and exit nodes in a chain of network nodes are most vulnerable; attackers can take over those nodes and thereby de-anonymize the messages. Therefore Tor does not use dynamically chosen entry nodes. The entry nodes – called "entry guards" – are chosen by the client from a list of well known entry nodes with a high transfer rate and a high availability.

The last part of the connection between the Tor exit node and the destination can be insecure and monitored by attackers. It is advised to use a secure connection via SSL/TSL between the source and destination over the Tor network.

> *TorButton has evolved to give considerable thought to fingerprint resistance and may be receiving the levels of scrutiny necessary to succeed in that project.*
> — [8, p. 14]

10. **T**he **O**nion **R**outing, see [18]

Tor is a useful service to anonymize the web traffic and hide the users' IP address, but it should be self-evident to use it with care. Oneself's behaviour must be adapted to some rules to achieve a high anonymity in the Internet.

A bundle[11] including the Tor software and a pre-configured web browser helps to get started with Tor easily. There are also some additional packages and tools for more experienced users.

3.2.2 Startingpage

"Startingpage" [20] is an extended secure version of Googles' search engine. It offers a proxy that relays the original search request to Google, draws a curtain over the search request and strips off all client identification information. As no identification information and IP addresses are saved this allows an anonymous search experience.

The provider of Startingpage "Ixquick" has been certified by *EuroPriSe*, a privacy initiative by the European Union. Ixquick offers the first and officially certified secure search engine.

The Startingpage service is available as a website with a Google-like appearance, or as a search engine entry in the Firefox browser search bar.

3.3 Browser Extensions

Browser extensions can be used to protect the user against threats from the Internet. The following extensions are examples for the Mozilla-based web browser Firefox. There are similar extensions for other modern browsers.

3.3.1 NoScript

NoScript [21] is a free extension for the web browser Firefox or other Mozilla-based browsers. This addon allows the execution of trusted active site elements e.g. JavaScript, Java, Flash, Silverlight or other plugins based on a whitelist. By default all non-known active site elements are blocked. This feature reduces security issues, masks the browsers fingerprint and decreases its uniqueness (see subsection 2.5). In addition it has also a powerful Anti-XSS[12] protection.

Since its start in 2005, *NoScript* has become a famous extensions for Firefox. It is a good advice to use *NoScript* to achieve a more secure browsing experience.

> *NoScript is a useful privacy enhancing technology that seems to reduce fingerprintability.*
> — [8, p. 14]

11. https://www.torproject.org/projects/torbrowser.html
12. **C**ross-**s**ite **s**cripting

3.3.2 BetterPrivacy

BetterPrivacy [22] is another Firefox extension to protect the user's browser against undeletable cookies – so called "Zombie-Cookies" (see subsection 2.1). For example flash cookies are stored in a system folder and thus protected against deletion by the browser. *BetterPrivacy* can detect these cookies and delete them. Normally the user won't even notice the extension: cookies are deleted either timer controlled or at browser shutdown. Newer Firefox versions have this functionality already built in. This feature reduces the trackability by third parties.

3.3.3 Ghostery

Ghostery [23] is able to detect web bugs (see subsection 2.2), tracking cookies (see subsection 2.1), and other kinds of tracking tools included into the current loaded website. The extension has a list with a lot of known advertisement and tracking web bugs or cookies in order to block and stop them from being loaded. If tracking content is recognized, the user will be informed by a small bubble in the browser's window. This extension is useful to protect the user's privacy and trackability against third party web bugs, but this extension is only as good as the included blacklist by the programmers.

3.3.4 GoogleSharing

A search engine may become a serious threat to a user's privacy as described in section 1 and shown in Figure 2. It is essential to protect the end-user, its search terms, and intentions against the search engine. "*GoogleSharing* is a system that mixes the requests of many different users together, such that Google is not capable of telling what is coming from whom." [24]. Therefore the proxy generates a pool of identities of known user-agents and uses one of them to relay the search request to the search engine. The original request is stripped off from all client identifying information by the proxy.

> *GoogleSharing is a special kind of anonymizing proxy service, designed for a very specific threat. It ultimately aims to provide a level of anonymity that will prevent Google from tracking your searches, movements, and what websites you visit.*
> — [24]

This extension captures the actual query and forwards the request through a proxy to the original server. Normally the user doesn't even notice that his request has been forwarded. The actual search flow is not interrupted, but only extended by a security feature.

3.3.5 HTTPS Everywhere

Today, many websites offer limited HTTPS [13] support. Links, scripts and other data in those pages are included with mixed protocols (HTTP, HTTPS). The Firefox extension *HTTPS Everywhere* [25] fixes this issue by altering links etc. from known websites to a secure connection over SSL/TSL if available in the extensions' whitelist. The user can also write own rules for websites not listed in the *HTTPS Everywhere* extension.

13. **H**ypertext **T**ransfer **P**rotocol **S**ecure – HTTP over SSL/TSL, see subsection 3.1

3.3.6 Ref Control

Browsing between different websites leaves tracks and useful information for third parties. The evildoer in this case is the so called "HTTP Referrer" sent by the browser, which tells a website from where the user is coming. It is easy to derive a user profile from this information. *Ref Control* [26] is another useful Firefox extension which can block HTTP Referrers by default. The user can also define own rules and thereby create a whitelists and blacklists for different websites.

4 Conclusion

The previous sections hopefully showed how serious the tracking issues is. Harmless looking websites can serve as information collecting and user tracking data kraken. User profiles can be derived from this data and sold for profit to well paying recipients. Sadly, this is no science-fiction and already happening.

Therefore, the motto is: shields up! Today there are a lot of known techniques (see section 3) and browser extensions (see subsection 3.3) to protect the web user and his traffic. The Firefox extension *NoScript* is useful to block undesired external tracking and maybe malicious scripts. An unintended side effect is that *NoScript* reduces the browsers' uniqueness and thus its fingerprint (see subsection 2.5). Therefore, you should install the *NoScript* extension. Initially, it may be a little bit disturbing to create a whitelist, but it's worth the effort.

> *We identified only three groups of browser with comparatively good resistance to fingerprinting: those that block JavaScript, those that use TorButton, and certain types of smartphone.*
> — [8, p. 16]

NoScript is adequate for a lot of users. In order to hide your IP address from a search engine a proxy service like *Startingpage* or *GoogleSharing* is required. However, to mask your IP address and make your traffic completely anonymous a proxy service like the *Tor Project* is more useful. If you feel insecure while searching, you should use a proxy service or an extended secure search engine like *Startingpage*.

For any kind of sensitive data e.g. personal information, login, or banking data, make sure to use a secure connection over SSL/TSL (see subsection 3.1). In Firefox you can check this by clicking on the websites' icon at the left of the address bar.

Keep in mind: your system is only as secure as your weakest member in the whole chain!

REFERENCES

[1] Wikipedia, "DMZ (computing) — wikipedia, the free encyclopedia," 2011, [Online; accessed 11-July-2011]. [Online]. Available: http://en.wikipedia.org/wiki/DMZ_(computing)

[2] F. O. for Information Security (BSI), "IT-Grundschutz Catalogues," July 2011. [Online]. Available: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html

[3] T. H. Security, "RSA break-in: it was the Flash Player's fault," 4 April 2011. [Online]. Available: http://h-online.com/-1221057

[4] ——, "PSN hack (Sony): Personal data of millions of customers stolen," 27 April 2011. [Online]. Available: http://h-online.com/-1233209

[5] ——, "Hackers break into Lockheed Martin," 29 May 2011. [Online]. Available: http://h-online.com/-1251978

[6] ——, "Anonymous hacks another US government contractor," 12 July 2011. [Online]. Available: http://h-online.com/-1277746

[7] B. R. . C. M. G. Corporate Trust, "Studie: Industriespionage – Die Schäden durch Spionage in der Deutschen Wirtschaft," 2007.

[8] E. F. F. Peter Eckersley, "How unique is your web browser?" May 2010. [Online]. Available: http://panopticlick.eff.org

[9] Wikipedia, "Web bug — wikipedia, the free encyclopedia," 2011, [Online; accessed 19-July-2011]. [Online]. Available: http://en.wikipedia.org/wiki/Web_bug

[10] ——, "Geotargeting — wikipedia, the free encyclopedia," 2011, [Online; accessed 19-July-2011]. [Online]. Available: http://en.wikipedia.org/wiki/Geotargeting

[11] R. C. Hodgin, "YouTube blocks GEMA music videos in Germany," April 2009. [Online]. Available: http://www.tgdaily.com/business/41913-youtube-blocks-gema-music-videos-in-germany

[12] U. H. P. Tecrux, "Ipv4 to exhaust by 2nd feb," January 2011. [Online]. Available: http://www.tecrux.com/2011/01/23/ipv4-to-exhaust-by-2nd-feb-report/

[13] C. Parsons, "IPv6 and the Future of Privacy," March 2010. [Online]. Available: http://www.christopher-parsons.com/blog/technology/ipv6-and-the-future-of-privacy/

[14] P. Schaar, "IPv6 – Wo bleibt der Datenschutz?" June 2011. [Online]. Available: https://www.bfdi.bund.de/bfdi_forum/showthread.php?2393-IPv6---Wo-bleibt-der-Datenschutz

[15] T. H. Security, "IPv6: Smartphones compromise users' privacy," January 2011. [Online]. Available: http://h-online.com/-1169708

[16] heise Netze, "Deutsche Telekom konkretisiert IPv6-Pläne," October 2010. [Online]. Available: http://heise.de/-1102458

[17] S. Thomas, *SSL & TLS Essentials: Securing the Web*. John Wiley & Sons Inc., 2000.

[18] "The tor project – anonymity online." [Online]. Available: https://www.torproject.org

[19] Wikipedia, "Onion routing — wikipedia, the free encyclopedia," 2011, [Online; accessed 28-August-2011]. [Online]. Available: http://wikipedia.org/wiki/Onion_routing

[20] Ixquick, "Startingpage web search." [Online]. Available: https://startingpage.com

[21] G. Maone, "NoScript." [Online]. Available: http://noscript.net

[22] NettiCat, "BetterPrivacy."

[23] Evidon, "Ghostery." [Online]. Available: http://www.ghostery.com

[24] T. I. F. D. S. Thoughtcrime Labs, "GoogleSharing." [Online]. Available: http://www.googlesharing.net

[25] Electronic Frontier Foundation, "HTTPS Everywhere." [Online]. Available: https://www.eff.org/https-everywhere

[26] James Abbatiello, "Ref Control." [Online]. Available: https://addons.mozilla.org/firefox/addon/refcontrol/